XINFENG LI

38 Zheda Road, Xihu District, Hangzhou, Zhejiang, 310007, China
LetterLiGO.github.io, xinfengli@zju.edu.cn, Zhejiang University (QS Ranking: 44th)

RESEARCH

My research is broadly in the field of ML and CPS security, with a particular interest in safeguarding intelligent audio/vision systems, user privacy, as well as generative models against various forms of leaks and attacks. I work toward developing dependable and secure machine learning (ML) systems and am committed to making their applications for deployment in critical infrastructures and consumer electronics. In user-oriented contexts, my investigations also encompass the interplay between protecting user privacy and enhancing the usability of machine learning systems. In model-oriented scenarios, such as the use of generative models in model-as-a-service (MaaS) applications, my work involves regulating their behavior to align with societal responsibilities.

EDUCATION

Zhejiang University (ZJU), Ubiquitous System Security Lab. (USSLAB) *2019.9 - Present*
Advisor: Prof. Wenyuan Xu
Ph.D., Electrical Engineering 5-year Ranking: 1st/87
Research Field: Audio Machine Learning, AI Security, CPS Security

Zhejiang University (ZJU) *2015.9 - 2019.6*
Advisor: Prof. Wenyuan Xu
B.S., Automation GPA: 90.03/100; Ranking: 2nd/82

SELECTED AWARDS AND SCHOLARSHIPS

- Ph.D. Wang Guosong Scholarship (Highest Honor in EE College, Top 1%) ZJU, 2023
- Outstanding Graduate Student Scholarship (Top 2%) ZJU, 2023
- Duanwei Educational Foundation Scholarship (Top 5%) ZJU, 2022
- Outstanding Graduate Student Scholarship (Top 2%) ZJU, 2021
- Outstanding Graduate Student Officer Scholarship ZJU, 2020
- Outstanding Graduate of Edison Honor Class ZJU, 2019
- Top Ten Student of EE College of ZJU (10/3200) ZJU, 2018
- National Scholarship (Top 2%) ZJU, 2018
- B.E. Wang Guosong Educational Foundation Scholarship (Top 2%) ZJU, 2018
- 2018 Smart Car Competition (1st Prize in Zhejiang Province & 2nd Prize in Nation) 2018
- First-class Merits Scholarship (Top 3%) ZJU, 2018 & 2016

PUBLICATION

- **Xinfeng Li**, Chen Yan, Xuancun Lu, Xiaoyu Ji, Wenyuan Xu. *Inaudible Adversarial Perturbation: Manipulating the Recognition of User Speech in Real Time.* In Proceedings of Network and Distributed System Security Symposium, **NDSS 2024** Symposium **(Core A*, Big4)**

- **Xinfeng Li**, Xiaoyu Ji, and Chen Yan, Chaohao Li, Yichen Li, Zhenning Zhang, Wenyuan Xu. *Learning Normality is Enough: A Software-based Mitigation against the Inaudible Voice Attacks.* In Proceedings of 32nd **USENIX Security 2023** Symposium **(Core A*, Big4)**

- **Xinfeng Li**, Junning Ze, Chen Yan, Yushi Cheng, Xiaoyu Ji, Wenyuan Xu. *Enrollment-stage Backdoor Attacks on Speaker Recognition Systems via Adversarial Ultrasound.* IEEE Internet of Things Journal, **IoT-J (SCI, JCR-1, IF: 10.238)**

- **Xinfeng Li**, Zhicong Zheng, Chen Yan, Chaohao Li, Xiaoyu Ji, Wenyuan Xu. *Towards Pitch-Insensitive Speaker Verification via Soundfield.* IEEE Internet of Things Journal, **IoT-J (SCI, JCR-1, IF: 10.238)**

- Jiangyi Deng*, **Xinfeng Li***, Yanjiao Chen, Haiqin Weng, Yan Liu, Tao Wei, Wenyuan Xu. *CommandSense: Automating Shell Log Auditing with Proprietary Command Explanation System.* USENIX Symposium on Networked Systems Design and Implementation (**NSDI 2024**, *co-first authors, in submission)

- Zhicong Zheng, **Xinfeng Li**, Chen Yan, Xiaoyu Ji, Wenyuan Xu. *The Silent Manipulator: Practical and Inaudible Backdoor Attack against Speech Recognition Systems.* ACM multimedia **MM 2023 (Core A*)**

- **Xinfeng Li**, Chen Yan, Xiaoyu Ji, Wenyuan Xu. *A Software-based Mitigation against Inaudible Voice Attacks with Channel Awareness and Normality Guidance.* Transcations on Dependable and Secure Computing, **TDSC** (**SCI, JCR-1, IF: 6.791**, in submission)

- Guoming Zhang, Xiaoyu Ji, **Xinfeng Li**, Gang Qu, Wenyuan Xu. *EarArray: Defending against DolphinAttack via Acoustic Attenuation.* In Proceedings of **NDSS 2021** Symposium (**Core A*, Big4**)

- Ruiwen He, Xiaoyu Ji, **Xinfeng Li**, Yushi Cheng, Wenyuan Xu. *"OK, Siri" or "Hey, Google": Evaluating Voiceprint Distinctiveness via Content-based PROLE Score* In Proceedings of 31st **USENIX Security 2022** Symposium (**Core A*, Big4**)

- Xiaoyu Ji, Guoming Zhang, **Xinfeng Li**, Gang Qu, Xiuzhen Cheng, Wenyuan Xu. *Detecting Inaudible Voice Commands via Acoustic Attenuation by Multi-channel Microphones.* Transcations on Dependable and Secure Computing, **TDSC** (**SCI, JCR-1, IF: 6.791**)

- Ruiwen He, Yushi Cheng, Junning Ze, **Xinfeng Li**, Xiaoyu Ji, Wenyuan Xu. *Scoring Metrics of Assessing Voiceprint Distinctiveness based on Speech Content and Rate.* Transcations on Dependable and Secure Computing, **TDSC** (**SCI, JCR-1, IF: 6.791**)

- Junning Ze, **Xinfeng Li**, Yushi Cheng, Xiaoyu Ji, Wenyuan Xu. *UltraBD: Backdoor Attack against Automatic Speaker Verification Systems via Adversarial Ultrasound.* In the proceedings of 2022 IEEE 28th International Conference on Parallel and Distributed Systems, **ICPADS** (**Core B**)

- Yizhuo Gao, **Xinfeng Li**, Chaohao Li, Weinong Sun, Xiaoyu Ji, Wenyuan Xu. *VarASV: Enabling Pitch-variable Automatic Speaker Verification via Multi-task Learning.* In the proceedings of 2021 IEEE 5th Conference on Energy Internet and Energy System Integration, **EI2** (2021)

SELECTED PATENTS

- **Xinfeng Li**, Wenyuan Xu, Xiaoyu Ji, Bolun Ren. A Domain Adaptation-based Method for Detecting Inaudible Voice Attacks. ZL2021 10473965.2.

- Wenyuan Xu, **Xinfeng Li**, Xiaoyu Ji, Chen Yan. An Attention-enhanced Filtering Based Classification Enhancement Method for DolphinAttacks. ZL 2022 10194280.9.

- Wenyuan Xu, **Xinfeng Li**, Chen Yan, Xiaoyu Ji. A Memory Network-enhanced Variational Inference Method for Detecting DolphinAttacks. ZL 2022 10206415.9.
- Wenyuan Xu, Xiaoyu Ji, **Xinfeng Li**. Business Logic Consistency Analysis for Microgrid Controllers based on Sense Control Logic. ZL 2019 10882444.5.
- Wenyuan Xu, Chen Yan, Xiaoyu Ji, **Xinfeng Li**, Xuancun Lu. An Ultrasonic Channel Modeling Method, Electronic Device and Storage Medium. ZL 2023 10638870.0.
- Wenyuan Xu, Chen Yan, Xiaoyu Ji, **Xinfeng Li**, Xuancun Lu. Anti-Eavesdropping Ultrasonic Interference Sample Design Method, System and Device. ZL 2023 10653928.9.

SERVICE

Teaching Service.

- Artificial Intelligence Security (Undergraduate), Fall 2022

Review Activity

- IEEE Transactions on Dependable and Secure Computing (TDSC) 2022
- IEEE Internet of Things Journal (IoT-J) 2023
- IEEE S&P (Oakland) 2021, 2022
- USENIX Security Symposium 2021, 2022, 2023, 2024
- Network and Distributed System Security (NDSS) Symposium 2021, 2022, 2023, 2024
- ACM Conference on Computer and Communications Security (CCS) 2021, 2023

STUDENT ADVISING

Zhicong Zheng	B.S. Computer Science (now: USSLAB)	2022-Present
Zitong Chen	M.S. Electrical Engineering (now: USSLAB)	2023-Present
Yifan Zheng	B.S. Control Science Engineering (now: USSLAB)	2023-Present
Zhi Lv	B.S. Eletrical Engineering	2022-2023
Jingjing Zhong	B.S. Control Science Engineering	2022-2023
Yiran Chen	B.S. Control Science Engineering	2022-2023
Zhenning Zhang	B.S. Computer Science (now: Microsoft)	2021-2022
Yichen Li	B.S. Computer Science (now: Ph.D. at HKUST)	2021-2022